

11/17

PATENT APPLICATION
Docket No. MS1-326USC1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Hunnicutt et al.

Serial No.: 09/224,918

) Appeal No.

Confirmation No. 3147

Filed: January 4, 1999

For: Access Check System Utilizing
Cached Access Permissions

Examiner: Bradley Edleman

The Honorable Commissioner of Patents and Trademarks
Washington, D. C. 20231



22801

PATENT TRADEMARK OFFICE

BRIEF OF APPELLANT

The Applicants have filed a timely Notice of Appeal from the action of the Examiner in finally rejecting all of the claims that were considered in this application. This Brief is being filed under the provisions of 37 C.F.R. § 1.192. The Filing Fee of \$320.00, as set forth in 37 C.F.R. § 1.17(c), is submitted herewith.

REAL PARTY IN INTEREST

The real party in interest comprises Microsoft Corporation, Inc. by way of assignment from Hunnicutt et al., who is the named inventive entity and is captioned in the present brief, to the Microsoft Corporation, Inc. by way of an assignment document recorded at Reel/Frame 8110/0594 in the United States Patent and Trademark Office on August 14, 1996.

RECEIVED
JUN 26 AM 8:21
U.S. DEPT. OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON, D.C. 20535

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF CLAIMS

Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 are pending in the application.

STATUS OF AMENDMENTS

No amendment has been filed subsequent to the final Office action mailed on March 27, 2002 (hereinafter, the "FINAL").

SUMMARY OF INVENTION

The present invention provided an access-permission caching system for storing the last most recently generated access-permissions. If a request arrives at the server that is similar, in terms of the requesting user and the requested resource, to a previously processed request, then the system invention locates the previously generated access-permission in the access-cache. The requesting user's access-permission is therefore determined without opening the requested resource to read the associated access control list.

When a user logs-on to an operating system, the user supplies a user-name and password. If the operating system recognizes the user then a unique user-token is generated by the system and the user-token is added to a user-token cache. At subsequent log-ons by the same user, the system returns the same user-token from the user-token cache. Then, if the user has requested a resource, the system checks the access-cache to see if the requested resource has already been accessed by the

requesting user. If the requested resource has already been accessed by the requesting user then access to the resource is again provided by the system.

The access-cache contains access-permissions. Each access-permission relates to a previously processed resource request and contains the name of the requested resource and the user-name of the user that requested the resource. In an embodiment of the present invention, the access-cache contains an access-permission for each instance of a resource that has been accessed. In a further embodiment of the present invention the access-cache contains an access-permission for only the most-recent instance that a resource has been accessed. If the access-cache does not contain an access-permission containing the appropriate user-token and file-name, then a full access check is performed as described above with respect to existing access check systems. If upon performing the full access check it is determined that the requesting user has permission to access the requested resource, the system combines the name of the requested resource with the user-token of the requesting user into an access-permission and stores the access-permission in the access-cache. When this resource is specified in subsequent requests by the same user, the system will locate the relevant matching access-permission in the access-cache and return the matching access-permission to the server thereby indicating a positive result for the access check. The server then makes available to the user the requested resource.

When a user-token is removed from the user-token cache, the access-cache is scanned for all access-permissions containing the subject user-token and all occurrences are removed from the access cache. When a resource is changed, all access-permissions in the access-cache associated with the subject resource are removed from the access-cache.

(Except from Specification, Page 3, line 33 – Page 5, line 17)

ISSUES

1. Whether claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 satisfy the requirements of 35 U.S.C. § 112, ¶ 1, such that these claims contain subject matter which was described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention.
2. Whether claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 satisfies the requirements of 35 U.S.C. § 112, ¶ 2 for particularly and specificity so as to point out and distinctly claim the subject matter which the applicants regard as their invention.
3. Whether claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49 satisfy the requirements of 35 U.S.C. § 103(a) as being nonobvious over Wobber et al. (US Patent No. 5,235,642).
4. Whether claims 4, 5, 18 and 19 satisfy the requirements of 35 U.S.C. § 103(a) as being nonobvious over Wobber et al. (US Patent No. 5,235,642) in view of Carlson et al. (US Patent No. 5, 506,961).

GROUPING OF CLAIMS

There are five (5) separate grounds of rejection that are appealed herein:

- I. First Ground of Rejection: The grounds of the rejection based on 35 U.S.C. 112, first paragraph, directed toward pending Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 such that these claims stand or fall together as to this rejection.

II. Second Ground of Rejection: The grounds of the rejection based on 35 U.S.C. 112, second paragraph, directed toward pending Claims 1-36 and 41 such that these claims stand or fall together as to this rejection.

III. Third Ground of Rejection: The grounds of the rejection based on 35 U.S.C. 112, second paragraph, directed toward pending Claims 37-40 and 42-49 such that these claims stand or fall together as to this rejection.

IV. Fourth Ground of Rejection: The grounds of the rejection based on 35 U.S.C. 103(a) directed toward pending Claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49 such that these claims stand or fall together as to this rejection.

V. Fifth Ground of Rejection: The grounds of the rejection based on 35 U.S.C. 103(a) directed toward pending Claims 4, 5, 18 and 19 such that these claims stand or fall together as to this rejection.

ARGUMENT

First Ground of Rejection. Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 satisfy the requirements of 35 U.S.C. § 112, ¶ 1 so as to contain subject matter which was described in the specification in such a way as to reasonable convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

1. At pages 2-4, the FINAL rejects all pending claims under 35 U.S.C. 112, first paragraph, on the basis of an assertion set forth at paragraph No. 1 (hereinafter, the “Nonenablement Assertion”). An excerpt of the Nonenablement Assertion observes that:

“[t]he specification describes two separate processes. *** These two processes operate on some of the same data, but they are separate processes that occur independently of each other.

Each of the independent claims essentially combines these two separate steps into a single, if-then-else routine *** However, as explicitly stated in the specification, the steps of checking for alterations and flushing the cache occur on a *regular, periodic basis*. These steps occur separately from any access request, and there is no routine described in the specification that combines these two separate features. *** On (sic) step does not occur as a result of the other, as claimed.

Therefore, *** the claims include new matter that was not described in the specification at the time the application was filed ***.

(FINAL at Pages 2-4)

The Nonenablement Assertion protests the pending claims in their recitation of two (2) processes (hereinafter, respectively, the “FIRST PROCESS” and the “SECOND PROCESS”). The Applicants traverse and respectfully submit that the originally filed claims in the parent application, of which the present application is a continuation, recite a method that includes both of the FIRST PROCESS and the SECOND PROCESS. As such, these two (2) processes are not “separate processes that occur independently of each other” as alleged by the Nonenablement Assertion, but rather are two processes in a single method providing, respectively, access and access security to network resources.

2. The pending claims rejected under 35 U.S.C. § 112, first paragraph, find support in the originally filed Claim 1 and 18-22 of US Patent Application Serial No. 08/869,838, filed on August 14, 1996, now US Patent No. 5,889,952 (hereinafter, the “PARENT”), of which the present application is a continuation application.

In establishing a disclosure, applicant may rely not only on the description and drawing as filed but also on the original claims if their content justifies it. (MPEP 608.01 (I))

Original Claims 1 and 18-22 from the PARENT are as follows:

1. A machine-readable program storage device, tangibly embodying instructions executable by a computer to perform method steps for providing access to resources in a file system where access to said resources is controlled by said network server and users send requests to said network server for permission to access said resources, said method steps comprising:

receiving a first resource request from a one of said users whereby said one of said users requests to access a requested one of said resources;

determining, in response to said first resource request, that said one of said users has permission to access said requested resource;

generating, in response to successfully determining that said one of said users has permission to access said requested resource, an access-permission;

storing said access-permission in an access-cache wherein said access cache contains n of the last access-permissions generated, where n is a positive integer greater than 2;

providing access to said requested resource by said one of said users in response to successfully determining that said one of said users has permission to access said requested resource;

receiving a second resource request from a second one of said users to access said requested resource;

retrieving a one of said access-permissions stored in said access-cache in response to receipt of said second resource request wherein said second resource request necessitates the same access-permission as said access-permission stored in said access-cache; and

providing access to said requested resource by said second one of said users in response to said retrieving step.

18. A method according to claim 1 further comprising the steps of:
tracking security changes made to said network server; and
updating, in response to said tracking step, said access-cache to ensure the security of resources stored on said server.

19. A method according to claim 18 wherein said tracking step includes:
tracking changes made to a user-token cache wherein said user-token cache contains a unique user-token for each of said users that has logged on to said network server.

20. A method according to claim 19 wherein said updating step includes:
removing from said access-cache all said access-permissions containing said changed user-token.

21. A method according to claim 18 wherein said tracking step includes:
tracking changes made to said resources in said file system by storing a

resource name of a resource that has been changed.

22. A method according to claim 21 wherein said updating step includes: removing from said access-cache all said access-permissions containing a name of one of said changed resources.

A single method is recited in original Claim 1 and its dependent Claims 18-22. The FIRST PROCESS is recited in Claim 1 and the SECOND PROCESS is recited in Claims 18-22. The FIRST PROCESS recited in Claim 1 generates an “access permission” that is stored in “an access-cache”. The SECOND PROCESS recited in Claims 18-22 performs “tracking security changes” upon “said access-cache” with respect to “said access-permissions” which would not have been created in the access-cache but for the steps of Claim 1. Thus, the SECOND PROCESS recited in Claims 18-22 is inherently preceded by the FIRST PROCESS recited in Claim 1 as would be recognized by persons of ordinary skill. Accordingly, no new matter has been added.

By disclosing in a patent application a device that inherently performs a function or has a property, operates according to a theory or has an advantage, a patent application necessarily discloses that function, theory or advantage, even though it says nothing explicit concerning it. The application may later be amended to recite the function, theory or advantage without introducing prohibited new matter. *In re Reynolds*, 443 F.2d 384, 170 USPQ 94 (CCPA 1971); *In re Smythe*, 480 F. 2d 1376, 178 USPQ 279 (CCPA 1973).

3. The Nonenablement Assertion represents that the SECOND PROCESS is disclosed only as set forth in the specification, at Page 18, lines 11-13, namely that:

“[t]he processing steps 600-606 depicted in FIG. 6 are repeated on a regular, periodic basis to ensure the security of the resources of server 100.” (emphasis added)

Contrary to the Nonenablement Assertion, other disclosure in the specification does not so limit the SECOND PROCESS. To wit:

When a user-token is removed from the user-token cache, the access-cache is scanned for all access-permissions containing the subject user-token and all occurrences are removed from the access cache. When a resource is changed, all access-permissions in the access-cache associated with the subject resource are removed from the access-cache.

(Specification at Page 5, lines 11-17)

The foregoing passage from the specification discloses an embodiment in which the access-cache is changed after a user-token is removed or a resource is changed. The Nonenablement Assertion implies that change to the user-token cache will only be made during the SECOND PROCESS, but this point is not borne out by the specification. At Page 10, lines 20 through Page 11, line 4, it is disclosed that a user-token in the user-token cache can be removed or “over-written” during the FIRST PROCESS:

In a further embodiment of the present invention, access-cache 400 only contains an access-permission for the most recent instance of a file having been accessed. For example, FIG. 4 indicates two access permissions 403 and 405 for file name 300. *If access-permission 403 is the more recent of the two then it would have over-written access-permission 405* and there would be only a single access-permission for file 300 in access-cache 400. (emphasis added)

4. The Nonenablement Assertion denies the inherency of performing the SECOND PROCESS either regularly and/or periodically where the basis is the performance of the FIRST PROCESS. This is seen in the FIRST PROCESS where the user-token is removed from the user-token cache by an over writing operation (Specification at Page 5, lines 11-17, discussed above) and is also set forth at Page 14, lines 21-29:

If a user's access to the resources of server 100 is modified or eliminated, then the corresponding entry in the user-token cache is removed. When a user-token

is removed from user-token cache 200, the system of the present invention flushes all access-permissions in access-cache 400 containing the removed user-token. This eliminates the possibility of access-cache 400 allowing access to resources even after a user's access to server 100 has been modified or eliminated.

5. For the foregoing reasons, the Applicants respectfully assert that Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 are enabled in view of the specification and respectfully request that the Board overturn the rejection under 35 U.S.C. § 112, ¶ 1.

Second Ground of Rejection. Claims 1-36 and 41 satisfy the requirements of 35 U.S.C. § 112, ¶ 2 so as to particularly point out and distinct claim the subject matter which the Applicants regards as their invention.

1. The FINAL states, at Page 5, that all of Claims 1-36 and 41:

include if-then-else statements that do not logically flow from the preceding claim language. *** The step of "determining" should not include within it steps of removing or providing access to a user. Perhaps the result of the determination step would be to provide access, but these claims, as presently worded, actually include the removing and providing steps as part of the determination step. Therefore, claims *** must be cancelled ***.

The Applicants respectfully traverse the foregoing and request consideration of the following.

2. The test for indefiniteness is whether two requirements of 35 U.S.C. § 112, ¶ are met:

(1) the claims must set forth the subject matter that applicants regard as their invention; and (2) the claims must particularly point out and distinctly define the

metes and bounds of the subject matter that will be protected by the patent grant.
(M.P.E.P. § 2171)

The language of the rejected claims are sufficiently definite when read according to the commonly understood meaning of the language, and particularly when read in the context of the specification. When the terms of the limitations are given their ordinarily understood meanings, there is no ambiguity. Furthermore, the claims must be read in light of the specification, which more explicitly defines and illustrates the meaning of the rejected limitation.

3. The understanding of those of skill in the relevant arts must be examined with respect to the Second Ground of Rejection.

"[T]he definiteness of the language must be analyzed -- not in a vacuum, but always in light of the teachings of the prior art and of the particular application disclosure as it would be interpreted by one possessing the ordinary level of skill in the pertinent art." In re Moore, 439 F.2d 1232, 1235, 169 U.S.P.Q. 236 (CCPA 1971).

Independent Claim 1 is a "computer-readable medium" claim. Independent Claims 15 and 41 are method claims involving a computer network. Independent Claim 35 also involves computers. Computers execute programs that employ logic statements, thereby processing data. Common data processing employs numerous logic strings of 'if, then, else' logic queries. These logic strings are readily seen in the limitations of the rejected claims, some of which are patterned after the logic string 'determining if X, then Y, else Z', where Z can include further 'if/then' logic strings. These are neither esoteric nor uncertain concepts to one possessing the ordinary level of skill in the pertinent art.

The examination process is to interpret a claim in view of what its entirety would reasonably apprise those of ordinary skill in the relevant art as to its scope. Each Claim 1-36 and 41 lacks neither specificity nor particularity in that a review of each claim in its entirety apprises one of ordinary skill in the art of its scope and therefore serves the notice function required by 35 U.S.C. § 112, ¶ 2.

4. The FINAL, in essence, argues that a recited manipulative step can not properly recite included manipulative steps. Stated otherwise, a claim element having a sub-element fails for indefiniteness. The Applicants are unaware of any authority that maintains as indefinite any claim that recites a manipulative step that has an included manipulative step and the FINAL nowhere states any authority for this position. The rejection is therefore ungrounded in authority.

5. The Applicants respectfully assert that Claims 1-36 and 41 are clear and definite in view of the specification and in view of the ordinarily understood meaning of the rejected language and respectfully request that the Board overturn the Second Ground of Rejection.

Third Ground of Rejection. Claims 37-40 and 42-49 satisfy the requirements of 35 U.S.C. § 112, ¶ 2 so as to particularly point out and distinct claim the subject matter which the Applicants regard as their invention.

1. The FINAL states, at Page 5, that each of these rejected:

claims requires a step of checking if “the user is/was logically present.” It is unclear as to how an actual user can be logically present in a cache.

The Applicants respectfully traverse the foregoing and request consideration of the following. Those of ordinary skill in the electrical arts will readily recognize a difference between a user ‘being present’ and a user being “logically present”. The former implies an actual physical presence whereas the latter implies an electronic presence by virtue of logic. The basis for this common knowledge is that a memory cache is an electronic storage. Electronic storage in memory is understood in the electrical arts to be a function of logic. Logic uses indicators that are based in a binary system that identifies status: on/off, yes/no, zero/1, present/absent, etc. Logic indicators are used to characterize data maintained in an electronic memory. As such, the plain meaning of the recited limitation “logically” is readily understood, both with respect to when a “network user is logically removed” as recited in Claims 37-40, and with respect to when “the user was logically present” as recited in Claims 42-49.

2. The FINAL should properly interpret Claims 37-40 and 42-49 in view of what their respective entireties would reasonably apprise those of ordinary skill in the relevant art as to their respective scope. On this basis and that set forth above, these claims lack neither specificity nor particularity in that a review of these claims in the entirety apprise one of ordinary skill in the art of their scope, therefore serving the notice function required by 35 U.S.C. § 112 2nd paragraph.

3. In that rejected claims employ commonly used terms in the electric arts, the Applicants respectfully assert that Claims 37-40 and 42-49 satisfy the requirements of 35 U.S.C. § 112, ¶ 2 so as to particularly point out and distinct claim the subject matter which the Applicants regard as their invention. The Board is requested to overturn the Third Ground of Rejection.

Fourth Ground of Rejection. Claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49 satisfy the requirements of 35 U.S.C. § 103(a) so as to be non-obvious over Wobber et al. (US Patent No. 5,235,642). To best characterize the issue before the Board, a brief review of the prosecution history is in order.

1. In the Office action mailed on August 1, 2001 (hereinafter, the “PRIOR action”), Claims 4, 5, 9-13, 18, 19, and 23-27 were rejected as non-obvious over Wobber et al. (US Patent No. 5,235,642). The PRIOR action relied solely on alleged common knowledge in the art or alleged well known prior art to supply each and every claim limitation that is not taught by Wobber et al. (hereinafter, the “FIRST OFFICIAL NOTICE”).

2. In the next response after the PRIOR action, which was mailed on October 26, 2001 (hereinafter, the “RESPONSE”), the Applicants made a demand for evidence to rebut the position in the PRIOR action that limitations recited in claims 4, 5, 9-13, 18, 19, and 23-27 that were missing from Wobber et al. were well known. The RESPONSE set forth the demand by statements characterizing the FIRST OFFICIAL NOTICE as being:

- (i) in a rejection that “fails to give proper weight” for each and every recited limitation missing from Wobber et al. (RESPONSE at P. 23) The recited limitations were given little or no attention in the rejection and, due to the importance of these recitations, deserved the greater weight of a reference citation to show each as being prior art in their respective combinations; and
- (ii) without any “basis for common knowledge in the art”. (RESPONSE at P. 23) The PRIOR action gave no support for the basis for asserting that the missing limitations were readily found in the common knowledge in the art; and
- (iii) an “absence of support for the limitations now present in the independent claims” (RESPONSE at P. 24). The RESPONSE added new limitations to Claims 1, 15, 31, 35, 37, 39, 41, 42, 44, 46, 47, and 49. Plainly, the FIRST OFFICIAL NOTICE could not have addressed as prior art each of the limitations that had been newly added by way of claim amendments in the RESPONSE.

3. The FINAL was mailed in reply to the RESPONSE. The FINAL alleged that the RESPONSE, by setting forth the foregoing statements (i) through (iii), above, did not make a *de facto* demand for evidence with respect to the FIRST OFFICIAL NOTICE such that the FIRST OFFICIAL NOTICE was admitted as prior art by the Applicants. The Applicants here argue that, rather than being an admission of the FIRST OFFICIAL NOTICE as prior art, any reasonable interpretation of the RESPONSE with respect to the FIRST OFFICIAL must be seen as Applicants’ traversal and challenge to the use of the FIRST OFFICIAL NOTICE as prior art. By the Applicants’ stated protest, the Applicants plainly asserted that the unsupported FIRST OFFICIAL NOTICE lacks evidentiary weight to supply what the applied sole reference can’t. The RESPONSE mandated upon the Office an obligation to supply evidence of greater weight to supplement the lack of weight complained of. Moreover, the Applicants insisted that the PRIOR action had given “no basis for common knowledge in the art”, thus demanding evidence of such basis of those claim elements alleged to be prior art in the FIRST OFFICIAL NOTICE.

4. The RESPONSE amended Claims 1, 15, 31, 35, 37, 39, 41, 42, 44, 46, 47, and 49 by adding still more limitations. The FINAL found that Wobber et al. do not teach those new limitations added in the RESPONSE but did find the newly added limitations to also be common knowledge in the art or well known prior art (hereinafter, the “SECOND OFFICIAL NOTICE”).

5. In response to the SECOND OFFICIAL NOTICE, the Applicants respectfully make a demand for evidence or in the alternative, that an explanation be given as to why the demanded evidence is not required. Additionally, the Applicants preserve their right under the first demand for evidence for support of the FIRST OFFICIAL NOTICE; re-assert the first demand for evidence, and further notes that no such evidence has been tendered in the FINAL as to the FIRST OFFICIAL NOTICE.

6. By requiring a demand for evidence to be fashioned other than by the simple notice for same given in the RESPONSE, the FINAL exalts form over substance and trivializes the seriousness of the Applicants’ protests of the FIRST OFFICIAL NOTICE. The US Patent and Trademark Office has as its stated goal “to help our customers get patents”. In this, the FINAL serves neither this goal nor a fair determination of patentability.

7. The Applicants respectfully assert, in view of the foregoing, that the FINAL has not made out a *prima facie* case of obvious, or in the alternative, the pending claims

avoid the rejections, and that Claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49 satisfy the requirements of 35 U.S.C. § 103(a) so as to be non-obvious over Wobber et al. (US Patent No. 5,235,642). The Applicants respectfully request the Board to overturn the Fourth Ground of Rejection.

Fifth Ground of Rejection. Claims 37-40 and 42-49 satisfy the requirements of 35 U.S.C. § 103(a) so as to be non-obvious over Wobber et al. (US Patent No. 5,235,642) in view of Carlson et al. (US Patent No. 5, 506,961).

1. The teaching deficiencies noted above with respect to Wobber et al. are not taught by Carlson et al., and are unsupported FIRST OFFICIAL NOTICE and by the Second OFFICIAL NOTICE.

2. The arguments set forth in the Fourth Ground of Rejections are re-asserted for the Fifth Ground of Rejection.

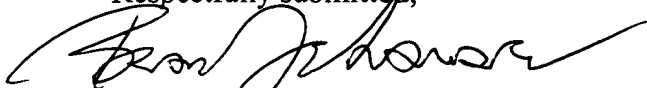
3. The Applicants respectfully assert, in view of the foregoing, that the FINAL has not made out a *prima facie* case of obvious, or in the alternative, the pending claims avoid the rejections, and that Claims 37-40 and 42-49 satisfy the requirements of 35 U.S.C. § 103(a) so as to be non-obvious over Wobber et al. (US Patent No. 5,235,642) in view of Carlson et al. (US Patent No. 5, 506,961). The Applicants respectfully request the Board to overturn the Fifth Ground of rejection.

CONCLUSION

The Applicants respectfully consider this application to be in condition for allowance and respectfully requests the Board to overturn the final rejection and that the Examiner passes this application to allowance.

Dated this 22ND day of August, 2002.

Respectfully submitted,



BRADLEY K. DESANDRO
Attorney for Applicant
Registration No. 34,521

LEE & HAYES PLLC
421 W. Riverside Avenue
Suite 500
Spokane, WA 99201
Telephone: (509) 324-9256 (Ext. 228)
Facsimile: (509) 323-8979

APPENDIX: CLAIMS ON APPEAL

1. A computer-readable medium having a plurality of executable instructions at least a subset of which, when executed, implement a method comprising:

upon receipt of an indication from a user having access to a computer network to access a resource on the computer network, checking a first memory, without performing a file open procedure upon a file in which are stored any access permissions of users for access to the resource, to determine:

if:

the requested resource is altered; or

a representation of the user has been removed from the first memory; or

any of the access permissions of the user for access to the requested

resource are altered:

then removing any access permissions from the first memory

allowing access to the requested resource by the user;

else, if:

the first memory indicates that the user has previously accessed the

resource:

then providing the user with access to the requested resource.

2. (Cancelled)

3. The computer-readable medium of claim 1 wherein the user is represented in the

first memory by a token.

4. The computer-readable medium of claim 3 wherein the token also represents a plurality of other users.

5. The computer-readable medium of claim 3 wherein the token also represents anonymous users.

6. (Cancelled)

7. The computer-readable medium of claim 1 wherein the resource is a file.

8. The computer-readable medium of claim 1 wherein the resource is a volume of files.

9. The computer-readable medium of claim 1 wherein the resource is a memory device.

10. The computer-readable medium of claim 29 wherein storing the information in the first memory comprises overwriting other information associated with the resource in the first memory.

11. The computer-readable medium of claim 10 wherein storing the information in

the first memory comprises writing a token for the user in the first memory over another token for another user that had last previous access to the resource.

12. (Cancelled)

13. (Cancelled)

14. The computer-readable medium of claim 1 wherein the request from the user indicates an operation to perform with respect to the resource, and further comprising:

checking the first memory to determine if the user may perform the operation with respect to the resource;

providing the user with access to the resource to perform the operation if the first memory indicates that the user may perform the operation with respect to the resource;

checking a second memory to determine if the user may perform the operation with respect to the resource if the first memory does not indicate that the user may perform the operation with respect to the resource;

providing the user with access to the resource if the second memory indicates that the user may perform the operation with respect to the resource; and

storing information in the first memory indicating that the user may perform the operation with respect to the resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the resource.

15. A method for providing access to a requested resource on a computer network, the method comprising:

checking a first memory, without performing a file open procedure upon a file in which are stored any access permissions of users for access to the requested resource, to determine:

if:

the requested resource is altered; or

a representation of a user has been removed from the first memory, where the user has access to the computer network and is requesting access to the requested resource; or

any of the access permissions of the user for access to the requested resource are altered:

then removing from the first memory any access permissions of the user that allow access to the requested resource by the user;

else, if:

the first memory indicates that the user has previously accessed the resource:

then providing the user with access to the requested resource.

16. (Cancelled)

17. The method of claim 15 wherein the user is represented in the first memory as a token.

18. The method of claim 17 wherein the token also represents a plurality of other users.

19. The method of claim 17 wherein the token represents anonymous users.

20. The method of claim 17 further comprising:
authorizing the user by checking a password provided by the user;
associating the token with the user after authorizing the user; and
using the token to check the first memory.

21. The method of claim 15 wherein the requested resource is a file.

22. The method of claim 15 wherein the requested resource is a volume of files.

23. The method of claim 15 wherein the requested resource is a memory device.

24. The method of claim 30 wherein storing the information in the first memory comprises overwriting other information associated with the requested resource in the first memory.

25. The method of claim 24 wherein storing the information in the first memory

comprises writing a token for the user in the first memory over another token for another user that had last previous access to the requested resource.

26. (Cancelled)

27. (Cancelled)

28. The method of claim 15 wherein the request from the user indicates an operation to perform with respect to the requested resource, and further comprising:

checking the first memory to determine if the user may perform the operation with respect to the requested resource;

providing the user with access to the requested resource to perform the operation if the first memory indicates that the user may perform the operation with respect to the requested resource;

checking a second memory to determine if the user may perform the operation with respect to the requested resource if the first memory does not indicate that the user may perform the operation with respect to the requested resource;

providing the user with access to the requested resource if the second memory indicates that the user may perform the operation with respect to the requested resource; and

storing information in the first memory indicating that the user may perform the operation with respect to the requested resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the requested resource.

29. A computer-readable medium according to claim 1, further comprising:

checking a second memory to determine if the user may access the resource if the first memory does not indicate that the user has previously accessed the resource;

providing the user with access to the resource if the second memory indicates that the user may access the resource; and

storing information in the first memory indicating that the user may access the resource if, after checking the second memory, the second memory indicates that the user may access the resource.

30. A method according to claim 15, further comprising:

checking a second memory to determine if the user may access the requested resource if the first memory does not indicate that the user has previously accessed the requested resource;

providing the user with access to the requested resource if the second memory so indicates;

and

storing information in the first memory indicating that the user may access the requested resource, if the second memory so indicates.

31. A method for controlling access to a requested resource on a computer network by a requesting user having access to the computer network, the method comprising:

checking a memory, without performing a file open procedure upon a file in which are stored any access permissions of users for access to the requested resource, to determine:

if:

the requested resource is altered; or

a representation of the user has been removed from the memory; or

any access permissions of the user for access to the requested resource are

altered:

then removing from the memory any access permissions of the user

for access to the requested resource;

else, if:

the memory indicates that the requesting user having access to the

computer network had previously accessed the requested resource:

then providing the requesting user with access to the requested resource.

32. A method according to claim 31, further comprising:

performing a file open procedure upon the file in which are stored any access permissions of users for access to the requested resource to determine if the requesting user may access the requested resource if the memory does not indicate that the requesting user has previously accessed the requested resource; and

providing the requesting user with access to the requested resource if the requested resource indicates that the requesting user may access the requested resource.

33. A method according to claim 32, further comprising:

storing information in the memory indicating that the user has previously accessed the requested resource.

34. A method according to claim 31, further comprising, prior to checking the memory, performing a preliminary memory check to determine if the requesting user has previously accessed the computer network.

35. A machine-readable program storage device embodying instructions executable by a computer to perform a method for providing access to a plurality of resources to a plurality of requesting users, wherein access to each said resource is controlled by a network server having a network memory, the method comprising:

receiving at the network server a resource request to access a requested resource of said plurality of resources from one said requesting user, wherein:

the network memory has stored therein which of said plurality of requesting users had accessed which of said plurality of resources; and

an access file has stored therein any access permissions of any users for access to the requested resource;

without opening the access file, checking the network memory to determine:

if:

the requested resource is altered; or

a representation of the requesting user has been removed from the network memory; or

any access permissions of the user for access to the requested resource are altered:

then removing from the network memory any access permissions of the user for access to the requested resource;

else, if:

the network memory indicates that the requesting user had previously accessed the requested resource:

then opening the requested resource to provide access to the requesting user.

36. The method of claim 35, the method further comprising, when the requesting user had not previously accessed the requested resource:

opening the access file;

checking the access file to determine if the requesting user may have access to the requested resource; and

if the check is affirmative, then providing said access.

37. A resource access system comprising:

a network, including a plurality of resources, for transmitting a resource request from a network user with access to the network for access to a requested resource of said plurality of resources; and

a network server, in communication with the network and a memory cache, for:

receiving the resource request;

checking the memory cache, without opening any of said plurality of resources, to determine whether:

the requested resource is altered; or

the network user is logically removed; or

any access permissions of the network user for access to the requested resource are altered;

if said checking is:

affirmative, then purging the memory cache of any access permissions of the network user for access to the requested resource;

negative, then determining if the network user's resource request had been previously granted and granting said access if the determining is affirmative.

38. The resource access system of claim 37, wherein granting said access further comprises opening the requested resource for the network user to have said access to the requested resource.

39. A program for a resource access system, the program being embodied on a computer-readable medium and executed on a server that provides access to resources on a network, the program comprising:

a code segment to receive a resource request for access to one said resource from a user having access to the network;

a code segment to check a memory cache, without opening any of said resources on the

network, to determine whether:

the requested resource is altered; or

the user is logically removed; or

any access permissions of the user for access to the requested resource are altered;

a code segment to purge the memory cache of any access permissions of the user for access to the requested resource if the check is affirmative;

a code segment to determine whether the user had previously been granted access to the requested resource; and

a code segment to grant said access if the check is negative and the determination is affirmative.

40. The program of claim 39 further comprising a code segment to open the requested resource for the user of the network to have said access to the requested resource if the check is affirmative.

41. A method for controlling access to a requested resource on a computer network by a requesting user, the method comprising:

checking a first memory, without opening the requested resource, to determine if the requesting user has previously accessed the network; and

if the requesting user has previously accessed the network:

providing the requesting user with access to the network;

checking a second memory, without opening the requested resource, to determine:

if:

the requested resource is altered; or
a representation of the requesting user has been removed
from the second memory; or

any access permissions of the user for access to the
requested resource are altered:

then removing from the second memory any access
permissions of the requesting user for access to the
requested resource;

else, if the second memory indicates that the requesting user has
previously accessed the requested resource, then providing the requesting
user with access to the requested resource;

else, if the requesting user has not previously accessed the
requested resource then opening the requested resource to determine if the
requesting user may access the requested resource and if the requested
resource indicates that the requesting user may access the requested
resource then providing the requesting user with access to the requested
resource.

42. A resource access determination method comprising:

receiving a request for an access to a resource from a user having had said access; and
deciding the request affirmatively based upon contents stored in a cache and without
opening the resource or contacting the user, if:

the requested resource was unaltered; and
the user was logically present; and
any access privileges of the user for access to the requested resource were
unaltered;
else purging contents of the cache of any access privileges of the user for access to the
requested resource.

43. The method as defined in Claim 42, further comprising, prior to said receiving:
receiving a request for an access to the resource from the user who had not previously
accessed the resource; and
obtaining any access privileges to the resource of the user without contacting the user.

44. A resource access determination method comprising:
receiving an initial request for an access to a resource from a user;
obtaining an access privilege of the user to the resource from a cache and without
contacting the user; and

if:

the user had the access privilege to the resource; and
the initially requested resource was unaltered; and

the user was logically present; and
any access privileges of the user for access to the requested resource were
unaltered;

then:

granting the initial request;

receiving subsequent requests for subsequent accesses to the
resource from the user; and

granting each said subsequent request without opening the resource
or contacting the user, but only if:

the subsequently requested resource was unaltered; and

the user was logically present; and

any access privileges of the user for access to the requested
resource were unaltered;

else purging the cache of any access privileges of

the user for access to the requested resource;

else purging the cache of any access privileges of the user for access to the requested
resource.

45. The method as defined in Claim 44, wherein:

granting the initial request further comprises caching the result of said obtaining said
access privilege of the user to the resource; and

granting each said subsequent request further comprises comparing each said subsequent

request with said cached result of said obtaining said access privilege of the user to the resource.

46. A resource access determination method comprising:

receiving a request for an access to a resource from a user having had said access; and

deciding the request affirmatively based upon contents stored in a cache, prior to contacting the user and without opening the resource, if:

- the requested resource was unaltered; and
- the user was logically present; and
- any requirements for access by the user to the resource were unaltered;

else purging contents of the cache of any requirements for access by the user to the resource.

47. In a system where resources are protected by access checks that are performed to confirm that a user meets any requirements for access to a particular resource, and where an access check is performed the first time that the user requests access to the particular resource to confirm that the user meets any requirements for access to the particular resource, a method for determining whether the user should have access to the particular resource, the method comprising:

- receiving a request from a user for access to a resource;
- checking the results of previous access request checks, which results are stored in a memory cache, to determine if the user has previously been allowed access to the

resource;

if:

the user has previously been allowed access to the resource and

the requested resource was unaltered; and

the user was logically present; and

any requirements for access by the user to the resource were unaltered;

then allowing access to the resource without performing an access check;

else purging contents stored in the memory cache of any requirements for access by the user to the resource.

48. The method as defined in Claim 47, wherein the results of previous access request checks are cached in a cache.

49. In a system where resources are protected by access checks that are performed to confirm that a user meets any requirements for access to a particular resource, where the requirements for each user to access each resource are stored in an access file, where an access check is performed the first time that the user requests access to the particular resource to confirm that the user meets any requirements for access to the particular resource, and where the access check that is performed the first time that the user requests access to the particular resource includes performing a file opening procedure upon the access file to determine the requirements for the user to access the particular resource, a method for determining whether the user should have access to the particular resource, the method comprising:

receiving a request from a user for access to a resource;

checking the results of previous access request checks, which results are stored in a memory cache, without opening the access file, to determine if the user has previously been allowed access to the resource;

if:

the user has previously been allowed access to the resource and

the resource was unaltered; and

the user was logically present; and

any requirements for access by the user to the resource were unaltered;

then allowing access to the resource without performing an access check;

else purging contents stored in the memory cache of any requirements for access by the user to the resource.